UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/075,471	02/13/2002	Jeffrey M. Ayars	41076.P001	7533

25943 7590 11/16/2005

SCHWABE, WILLIAMSON & WYATT, P.C.
PACWEST CENTER, SUITE 1900
1211 SW FIFTH AVENUE
PORTLAND, OR 97204

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/075,471	AYARS ET AL.	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 May 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Horstmann (6,044,469) in view of the article by M2 Presswire ("AMINO COMMUNICATIONS: Amino launches innovative approach to securing broadband communications; New technology provides digital rights protection for streaming content").

In reference to claims 1 and 29 Horstmann discloses a software publisher or distributor configurable software security mechanism (title). The apparatus disclosed by Hortmann is a tamper resistant digital content recovery module wherein the tamper resistance is provided by the protection wrapper, which runs code that performs the protection options, selected by the publisher (column 5 lines 2-30). The system of Hortmann discloses a plurality of plain text digital content rendering modules communicately coupled with each other in a hierarchical manner forming a hierarchy of modules (column 5 lines 54-59), with selective combinations of which to be selectively employed to render the recovered digital contents of corresponding types (column 6 lines 10-21), including one of the plain text digital content rendering modules occupying a root position (part 100 Fig. 5) of the hierarchy to exclusively receive the recovered digital contents to be rendered, of all types, from the tamper resistant digital content recovery module (column 6 lines 10-26). The system of Horstman includes one or more storage units to

store said tamper resistant module and said plurality of plain text digital content rendering modules (column 6 lines 5-10); and a processor coupled with the one or more storage units to execute the tamper resistant module and the plurality of plain text digital content rendering modules (column 6 lines 6-22).

Although Horstman discloses recovering protected digital contents, Horstman does not expressly disclose a system to recover protected digital contents of various types in an obfuscated manner.

The article by the M2 Presswire discloses a system that varies the level of encryption in real time depending upon the type and value of content or transaction. Therefore the system recovers protected digital contents in an obfuscated manner and the digital content is of various types (Full Text paragraphs 2-3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to recover protected digital contents of various types in an obfuscated manner as disclosed by the article by M2 Presswire in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because combining proven techniques minimizes the risk to content dynamically without compromising performance.

Claims 2-28 and 30-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Horstmann in view of the article by M2 Presswire as applied to claims 1 and 29 above, and further in view of Graunke et al (5, 991, 399).

In reference to claim 12, Horstmann discloses a software publisher or distributor configurable software security mechanism (title). The system comprises a root one of a plurality of hierarchically organized plain text digital content rendering modules collectively equipped to render digital contents requesting a tamper resistant digital content recovery module to recover a first protected digital content (column 5 lines 54-59). The tamper resistant digital content recovery module recovering the first protected digital content (part 100 Fig. 5), and transferring the recovered first digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules (column 6 lines 10-21), and said root one in conjunction with first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said first digital content (column 6 lines 10-21),

Although Horstman discloses recovering protected digital contents, Horstman does not expressly disclose a system to recover protected digital contents of various types in an obfuscated manner.

The article by the M2 Presswire discloses a system that varies the level of encryption in real time depending upon the type and value of content or transaction. Therefore the system recovers protected digital contents in an obfuscated manner and the digital content is of various types (Full Text paragraphs 2-3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to recover protected digital contents of various types in an obfuscated manner as disclosed by the article by M2 Presswire in the system of Horstman. One of ordinary skill in the

art would have been motivated to do this because combining proven techniques minimizes the risk to content dynamically without compromising performance.

Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the module has not been compromised. Although the claim recites, "...rendering modules has not been comprised..." the examiner assumes that the applicant meant compromised. Horstman further does not disclose the root verifying an immediate downstream module is uncompromised before transferring the first digital content to the immediate downstream module to further the rendering of the first digital content.

Grauke discloses a method for securely distributing a conditional use private key to a trusted entity on a remote system (abstract). The system of Graunke determines if the system is a trust worthy player (software) before providing the user with the key and therefore access to digital content (column 3 line 53 to column 4 line 7). In the case that the player is compromised the player does not have the ability to perform the cryptographic operation (column 4 lines 7-14).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because the integrity of the trusted player is correlated to its ability to perform a cryptographic operation using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

In reference to claims 18 and 25 Horstmann discloses a software publisher or distributor configurable software security mechanism (title). The apparatus disclosed by Hortmann is a tamper resistant digital content recovery module wherein the tamper resistance is provided by the protection wrapper, which runs code that performs the protection options, selected by the publisher (column 5 lines 2-30). The system of Hortmann discloses a plurality of plain text digital content rendering modules communicately coupled with each other in a hierarchical manner forming a hierarchy of modules (column 5 lines 54-59), with selective combinations of which to be selectively employed to render the recovered digital contents of corresponding types (column 6 lines 10-21), including one of the plain text digital content rendering modules occupying a root position (part 100 Fig. 5) of the hierarchy to exclusively receive the recovered digital contents to be rendered, of all types, from the tamper resistant digital content recovery module (column 6 lines 10-26). The system of Horstman includes one or more storage units to store said tamper resistant module and said plurality of plain text digital content rendering modules (column 6 lines 5-10); and a processor coupled with the one or more storage units to execute the tamper resistant module and the plurality of plain text digital content rendering modules (column 6 lines 6-22).

Although Horstman discloses recovering protected digital contents, Horstman does not expressly disclose a system to recover protected digital contents of various types in an obfuscated manner.

The article by the M2 Presswire discloses a system that varies the level of encryption in real time depending upon the type and value of content or transaction. Therefore the system

recovers protected digital contents in an obfuscated manner and the digital content is of various types (Full Text paragraphs 2-3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to recover protected digital contents of various types in an obfuscated manner as disclosed by the article by M2 Presswire in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because combining proven techniques minimizes the risk to content dynamically without compromising performance.

Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the module has not been compromised. Horstman further does not disclose the root verifying an immediate downstream module is uncompromised before transferring the first digital content to the immediate downstream module to further the rendering of the first digital content.

Grauke discloses a method for securely distributing a conditional use private key to a trusted entity on a remote system (abstract). The system of Graunke determines if the system is a trust worthy player (software) before providing the user with the key and therefore access to digital content (column 3 line 53 to column 4 line 7). In the case that the player is compromised the player does not have the ability to perform the cryptographic operation (column 4 lines 7-14).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke in the system

of Horstman. One of ordinary skill in the art would have been motivated to do this because the integrity of the trusted player is correlated to its ability to perform a cryptographic operation using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

In reference to claims 2 and 30 Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the module has not been compromised. Horstman further does not disclose the root verifying an immediate downstream module is uncompromised before transferring the first digital content to the immediate downstream module to further the rendering of the first digital content.

Grauke discloses a method for securely distributing a conditional use private key to a trusted entity on a remote system (abstract). The system of Graunke determines if the system is a trust worthy player (software) before providing the user with the key and therefore access to digital content (column 3 line 53 to column 4 line 7). In the case that the player is compromised the player does not have the ability to perform the cryptographic operation (column 4 lines 7-14).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because the integrity of the trusted player is correlated to its ability to perform a cryptographic operation using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

In reference to claims 3, 5-7, and 19-20 Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the content rendering module.

Grauke discloses a method for securely distributing a conditional use private key to a trusted entity on a remote system (abstract). The system of Graunke determines if the system is a trust worthy player (software) before providing the user with the key and therefore access to digital content (column 3 line 53 to column 4 line 7). The system of Graunke includes a tamper resistant module is equipped to verify the plain text digital content rendering module (Fig. 2). The verification of the module is in response to request from the tamper resistant module (column 4 lines 5-7).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because the integrity of the trusted player is correlated to its ability to perform a cryptographic operation using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

In reference to claims 4, 8, 13-15, 21, 26, and 31 Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the content rendering module.

Grauke discloses a method wherein the tamper resistant module is equipped to verify the plain text digital content rendering module occupying the root position of the hierarchy by verifying a signature of the plain text digital content rendering module occupying the root position.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because the integrity of the trusted player is correlated to its ability to perform a cryptographic operation using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

In reference to claims 8, 22, and 32, wherein the digital content of various types comprises streaming media contents of a plurality of media, and of a plurality of format types.

The article by the M2 Presswire discloses a system that varies the level of encryption in real time depending upon the type and value of content or transaction. Therefore the system recovers protected digital contents in an obfuscated manner and the digital content is of various types (Full Text paragraphs 2-3). The digital content disclosed includes all types of multimedia, for data, video , audio, news feeds and web pages (Full Text paragraphs 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to recover protected digital contents of various types in an obfuscated manner as disclosed by the article by M2 Presswire in the system of Horstman. One of ordinary skill in the

art would have been motivated to do this because combining proven techniques minimizes the risk to content dynamically without compromising performance.

In reference to claims 10 and 23 wherein the apparatus is a selected one of a wireless mobile phone, a palm sized personal digital assistant, a notebook computer, a set-top box, a desktop computer, a single processor server, a multi-processor server, and a cluster of coupled systems (column 5 lines 1-7).

In reference to claims 11 and 24 wherein a first subset of the plain text digital content rendering modules are member modules of a first application domain, and a second subset of the plain text digital content rendering modules are member modules of a second application domain.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to render modules are member modules of a second application domain. One of ordinary skill in the art would have been motivated to do this because dividing modules by domain is an easy and convenient method of

In reference to claim 33 wherein the recordable medium is a selected one of a magnetically recordable medium and an optically recordable medium.

In reference to claims 16 and 28 wherein the method further comprises the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module to recover a second protected digital content of the same first type; the tamper resistant digital content recovery module verifying that said root one of the plurality of hierarchically organized plain text digital content rendering modules

has not been comprised; the tamper resistant digital content recovery module recovering the second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules; and said root one in conjunction with the same first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with each of said root and same non-leaf ones, if any, of said first at least one other one of said plurality of hierarchically organized digital content rendering modules verifying an immediate downstream module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

Horstman discloses a system with the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module (Fig. 5). The system is used to recover digital content and therefore recovers a second protected digital content of the same first type. The tamper resistant digital content recovery module recovering the second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules (column 6 lines 10-22). Wherein the protected digital content is transferred to protector, which then runs the code selected using the software protection parameters.

Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the module has not been compromised. Horstman further

does not disclose the root verifying an immediate downstream module is uncompromised before transferring the first digital content to the immediate downstream module to further the rendering of the first digital content.

Grauke discloses a method for securely distributing a conditional use private key to a trusted entity on a remote system (abstract). The system of Graunke determines if the system is a trust worthy player (software) before providing the user with the key and therefore access to digital content (column 3 line 53 to column 4 line 7). In the case that the player is compromised the player does not have the ability to perform the cryptographic operation (column 4 lines 7-14).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because the integrity of the trusted player is correlated to its ability to perform a cryptographic operation using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

In reference to claims 17 and 27 wherein the method further comprises the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module to recover a second protected digital content of the same first type; the tamper resistant digital content recovery module verifying that said root one of the plurality of hierarchically organized plain text digital content rendering modules has not been comprised; the tamper resistant digital content recovery module recovering the

second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules; and said root one in conjunction with the same first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with each of said root and same non-leaf ones, if any, of said first at least one other one of said plurality of hierarchically organized digital content rendering modules verifying an immediate downstream module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

Horstman discloses a system with the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module (Fig. 5). The system is used to recover digital content and therefore recovers a second protected digital content of the same first type. The tamper resistant digital content recovery module recovering the second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules (column 6 lines 10-22). Wherein the protected digital content is transferred to protector, which then runs the code selected using the software protection parameters.

Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the module has not been compromised. Horstman further does not disclose the root verifying an immediate downstream module is uncompromised before

transferring the first digital content to the immediate downstream module to further the rendering of the first digital content.

Grauke discloses a method for securely distributing a conditional use private key to a trusted entity on a remote system (abstract). The system of Graunke determines if the system is a trust worthy player (software) before providing the user with the key and therefore access to digital content (column 3 line 53 to column 4 line 7). In the case that the player is compromised the player does not have the ability to perform the cryptographic operation (column 4 lines 7-14).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke of the root module and the leaf modules of the system of Horstman. One of ordinary skill in the art would have been motivated to do this because the integrity of the trusted player is correlated to its ability to perform a cryptographic operation using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Thursday, November 10, 2005

Primary Examiner
Art Unit 2135